Putting NYDFS AI Cybersecurity Guidance Into Practice

By **Matthew Kohel and Ryan Gallagher** (November 8, 2024)

Matthew Kohel

Ryan Gallagher

On Oct. 16, the New York Department of Financial Services issued guidance and strategies for addressing cybersecurity risks arising from advancements in artificial intelligence.

While AI technology has, in many cases, positively affected businesses, it has also opened the door to a myriad of opportunities for cyber criminals to infiltrate secure information systems containing nonpublic information, or NPI.

The NYDFS explained that the guidance does not impose any new requirements beyond the obligations already in the cybersecurity regulation codified at Title 23 of the New York Codes, Rules and Regulations, Part 500; rather, the guidance is meant to explain how covered entities[1] should use the framework in the cybersecurity regulation to assess and mitigate cyber risks associated with AI.[2]

Biggest Risks From Use of AI

The guidance focuses on four main risks related to the use of AI.

AI-Enabled Social Engineering

AI-enabled social engineering is one of the most significant threats to covered entities because AI can be used to target individuals in an attempt to lure or convince them to disclose NPI, or to take action that they are otherwise unauthorized to take, such as making wire transfers to fraudulent accounts.

AI-Enhanced Cybersecurity Attacks

AI allows threat actors to speed up cyberattacks and execute them on a much larger scale, given AI's ability to quickly scan and analyze voluminous amounts of information and identify security vulnerabilities. These AI technologies give even inexperienced threat actors a tool to launch calculated attacks, increasing their frequency and severity.

Exposure or Theft of Vast Amounts of NPI

This threat concerns the large collection and storage of NPI, including biometric data such as facial and fingerprint recognition, placing a larger target on data collection systems. Threat actors are capable of using biometric data to impersonate authorized users to bypass multifactor authentication, gain access to NPI and generate AI-enabled social engineering to target other users.

Increased Vulnerabilities Due to Third-Party, Vendor or Other Supply Chain Dependencies

These dependencies present concerns beyond internal cybersecurity measures of covered entities because security vulnerabilities can be exploited down the supply chain, potentially exposing the covered entity's NPI and giving way to broader cyberattacks through the

organization's network and chain of commerce.[3]

Mitigating the Risks

It should go without saying that covered entities should assess AI-related risks in their own design, development and use of AI; AI technologies utilized by third-party service providers that have access to their data; and susceptibilities stemming from AI applications, especially public platforms such as ChatGPT.

As part of a cybersecurity program required under the cybersecurity regulations, in the course of conducting any required risk assessment, covered entities should evaluate AI-related cyber risks to determine necessary updates to cybersecurity, privacy and data governance policies, including incident response and business continuity plans. Additionally, it is important to maintain strong contracts with third-party service providers and vendors to address unauthorized access of NPI, including duties to cooperate and broad indemnification provisions.

Pursuant to the cybersecurity regulations, a covered entity's cybersecurity policies should require access controls, such as encryption technologies and multifactor authentication, that require authorized users to properly authenticate their identities. Also, internal training and awareness remain key parts of a robust cybersecurity program, and employee training should include guidelines for monitoring new security vulnerabilities that may arise from the activities of authorized users and effective data management practices.

Employee training for both covered entities and their third-party service providers is one of the most vital countermeasures to cybersecurity threats, as AI-related cyberattacks are becoming increasingly more sophisticated and difficult to spot. AI-enabled social engineering appears to have become one of the most effective methods for threat actors to infiltrate information systems due to a lack of employee training or the failure to sufficiently monitor the activities of authorized users.

While individuals may find multifactor authentication to be somewhat tedious, it is an important part of a robust cybersecurity program. Thus, managing and monitoring authorized users will help mitigate cyber risks and protect information systems.

Beginning Nov. 1, 2025, covered entities will be required under the cybersecurity regulations to maintain and update data inventories.[4] This means that covered entities will be required to implement policies and procedures to ensure that their asset inventories are appropriately maintained in their information systems. The cybersecurity regulations mandate that, at a minimum, these policies and procedures include:

> (1) a method to track key information for each asset; including, as applicable, the following:
>
> > (i) owner;
> >
> > (ii) location;
> >
> > (iii) classification or sensitivity;
> >
> > (iv) support expiration date;
> >
> > (v) recovery time objectives; and

(2) the frequency required to update and validate the covered entity's asset inventory.[5]

Note, the changes will require additional policies and procedures governing the proper disposal of NPI in a secure manner.

AI technology is continuing to be adopted within organizations and by threat actors, and each environment presents its own risks and requires its own mitigation measures. The accessibility and evolution of AI tools that can be used to exploit cybersecurity vulnerabilities makes it difficult to keep up with the challenges posed by this technology, and AI is being used to increase the frequency and sophistication of attacks on organizations.

Covered entities need to be proactive in assessing the risks presented by the use of AI both internally and externally. They must also be proactive in developing the policies, procedures and mitigation strategies outlined in the guidelines to protect their information systems and NPI, and mitigate severe disruptions to business.

Covered entities must also ensure that all third-party providers are contractually obligated to implement cyberattack countermeasures that meet with the covered entity's approval and sufficiently protect its information systems through strong indemnification provisions, representations and warranties.

Lawyers representing covered entities, and even small business organizations, should counsel their clients on the application of the cybersecurity regulations and the foregoing guidance, along with the risks of utilizing AI technology and the importance of implementing robust cybersecurity programs.

Matthew D. Kohel is a partner and Ryan E. Gallagher is an associate at Saul Ewing LLP.

[1] Covered entity is defined in 23 NYCRR § 500.1(e) as

> any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies.

[2] https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks.

[3] Id.

[4] See 23 NYCRR Part 500.13.

[5] Id at (a)(1-2).